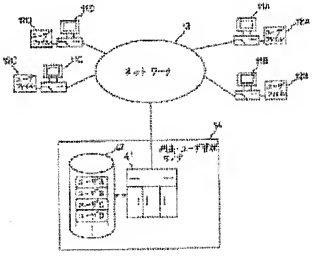
USER LIMITING METHOD IN ELECTRONIC ACCOUNT SETTLEMENT SYSTEM

Publication number: JP10143556 (A)
Publication date: 1998-05-29
Inventor(s): OCHIAI YUJI
Applicant(s): CARD KK U
Classification:
- international: ***G06Q20/00; G06Q10/00; G06Q50/00;*** **G06Q20/00; G06Q10/00; G06Q50/00;** (IPC1-7): G06F17/60
- European:
Application number: JP19960298826 19961111
Priority number(s): JP19960298826 19961111

Abstract of **JP 10143556 (A)**

PROBLEM TO BE SOLVED: To limit a user and to secure high security by making a balance /user management center allow account settlement when the final history information of a user file and the final history information of a data base are matching. SOLUTION: At the time of receiving a user authentication message and recognizing that a user ID and an electronic signature are normal, the management device 41 of a management center 14 confirms the history information of the received message by reading the final history information from a file corresponding to the user inside the data base 42 and comparing it with the received message. Then, in the case that a confirmed result is normal, the management device 41 allows the account settlement accompanying various electronic business transactions by the user.; Thereafter, at the time of confirming that the user is provided with a balance at the point of time of the account settlement, the management device 41 executes the electronic signature to the new balance information, records it in the file inside the data base 42 as the final history information and sends it through a network 13 to a pertinent terminal 11A. As a result, the history information of the user file is updated.



(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（A）**　(11)特許出願公開番号

特開平10－143556

(43)公開日　平成10年(1998)５月29日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｇ０６Ｆ　17/60		Ｃ０６Ｆ　15/21	３４０Ｂ

審査請求　未請求　請求項の数３　ＯＬ　（全　８　頁）

(21)出願番号　特願平8－298826

(22)出願日　平成８年(1996)11月11日

(71)出願人　33300/868
株式会社ユーカード
東京都渋谷区元代々木町30－13

(72)発明者　落合　祐二
東京都渋谷区元代々木町30－13　日交元代々木ビル　株式会社ユーカード内

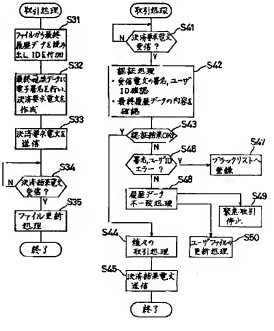
(74)代理人　弁理士　山川　政樹

(54)【発明の名称】　電子決済システムにおける利用者限定方法

(57)【要約】

【課題】　電子商取引を行う場合に高セキュリティを確保する。

【解決手段】　ネットワーク１３を介した電子商取引における決済時には、ユーザ端末１１はユーザファイル１２内の最終履歴データを管理センタ１４へ送信し、管理センタ１４ではこのデータを受信してデータベース４２内のユーザ端末１１に対応する最終履歴データとの一致を確認することでその決済を許容する。この結果、電子商取引を行う場合にその利用者を限定することができ、従って高セキュリティを確保できる。



【特許請求の範囲】
【請求項1】　ネットワークと、ネットワークに接続されると共にデータベースを有し各ユーザの残高の管理を行う残高・ユーザ管理センタと、ネットワークに接続され各ユーザがそれぞれ用いる各端末と、各端末に設けられ各ユーザの取引履歴情報を各個に記録するユーザファイルとからなり、残高・ユーザ管理センタでは、ユーザの電子商取引に伴う決済の都度、前記データベース内の対応のユーザのファイルの残高を更新し、かつこの更新情報を端末側へ送信して前記ユーザファイルを更新する電子決済システムであって、
前記電子商取引に伴う決済時に前記端末は前記ユーザファイルの最終履歴情報を前記残高・ユーザ管理センタに送信し、前記残高・ユーザ管理センタはこのユーザファイルの最終履歴情報と前記データベースの最終履歴情報とが一致するときに前記決済を許容することを特徴とする電子決済システムにおける利用者限定方法。
【請求項2】　請求項1において、
予めバックアップファイルを前記端末に設けて取引履歴情報をバックアップすると共に、前記残高・ユーザ管理センタからユーザファイルの最終履歴情報とデータベースの最終履歴情報との不一致が通知された場合、前記端末は前記バックアップファイルの取引履歴情報を残高・ユーザ管理センタへ送信しユーザファイルを更新することを特徴とする電子決済システムにおける利用者限定方法。
【請求項3】　請求項1において、
前記残高・ユーザ管理センタは履歴情報に自身の署名鍵を用いて電子署名を行い前記端末へ送信してユーザファイルに記録させ、前記端末はユーザファイル内の履歴情報に自身のＩＤを付加すると共にＩＤが付加された履歴情報に自身の署名鍵を用いて電子署名を行い前記残高・ユーザ管理センタへ送信し、履歴情報の正否を検証させることを特徴とする電子決済システムにおける利用者限定方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、電子決済システムにおける利用者限定方法に関する。
【０００２】
【従来の技術】マルチメディア技術の進歩やインターネット等のネットワークの普及により、電子商取引（エレクトロニック・コマース）が現実化しつつある。こうしたネットワークを介して各ユーザが電子商取引を行う場合、各ユーザの残高の管理を行う残高・ユーザ管理センタをネットワークに接続すると共に、各ユーザでは取引履歴を記録するユーザファイルを各個に設け、残高・ユーザ管理センタでは、ユーザの取引に伴う決済の都度、対応のユーザのファイルの残高を更新し、かつこの更新情報をユーザ側へ送信してユーザファイルを更新させるような電子決済システムが検討されている。
【０００３】
【発明が解決しようとする課題】こうした電子決済システムではインターネット等のネットワークを介在して不特定多数間で電子商取引が行われるため、他人に勝手に利用される恐れがあり、従って本人認証等のセキュリティには万全の体制をとることが要望されている。従って本発明は、電子決済システムにおいて高セキュリティを確保することを目的とする。
【０００４】
【課題を解決するための手段】このような課題を解決するために本発明は、ネットワークと、ネットワークに接続されると共にデータベースを有し各ユーザの残高の管理を行う残高・ユーザ管理センタと、ネットワークに接続され各ユーザがそれぞれ用いる各端末と、各端末に設けられ各ユーザの取引履歴情報を各個に記録するユーザファイルとからなり、残高・ユーザ管理センタでは、ユーザの電子商取引に伴う決済の都度、データベース内の対応のユーザのファイルの残高を更新し、かつこの更新情報を端末側へ送信してユーザファイルを更新する電子決済システムであって、電子商取引に伴う決済時に端末はユーザファイルの最終履歴情報を残高・ユーザ管理センタに送信し、残高・ユーザ管理センタはこのユーザファイルの最終履歴情報とデータベースの最終履歴情報とが一致するときに上記決済を許容するようにした方法である。従って、電子商取引を行う場合にその利用者を限定することができ、その結果高セキュリティを確保できる。また、予めバックアップファイルを端末に設けて取引履歴情報をバックアップすると共に、残高・ユーザ管理センタからユーザファイルの最終履歴情報とデータベースの最終履歴情報との不一致が通知された場合、端末はバックアップファイルの取引履歴情報を残高・ユーザ管理センタへ送信しユーザファイルを更新するようにした方法である。従って、ユーザファイル内の履歴データの紛失や破損等が生じた場合でもこれを復旧して決済を行うことができる。また、残高・ユーザ管理センタは履歴情報に自身の署名鍵を用いて電子署名を行い端末へ送信してユーザファイルに記録させ、端末はユーザファイル内の履歴情報に自身のＩＤを付加すると共にＩＤが付加された履歴情報に自身の署名鍵を用いて電子署名を行い残高・ユーザ管理センタへ送信し、履歴情報の正否を検証させるようにした方法である。従って、電子決済システムにおいてより高いセキュリティ性を確保できる。
【０００５】
【発明の実施の形態】以下、本発明について図面を参照して説明する。図１は本発明を適用した電子決済システムの構成を示すブロック図である。同図において、１１Ａ～１１Ｄは電子商取引時に各ユーザＡ～Ｄが各個に使用するユーザ端末、１２Ａ～１２Ｄは各ユーザ端末１１Ａ～１１Ｂに接続され、ユーザの取引履歴情報を記録す

るユーザファイル、１３はインタネット等のネットワーク、１４は残高・ユーザ管理センタ（以下、管理センタ）である。管理センタ１４には、管理装置４１とデータベース４２とが設けられ、データベース４２には各ユーザＡ～Ｄの取引履歴情報が各個に記録されるファイルが設けられている。

【０００６】図２はユーザファイル１２の構成を示す図であり、上述した取引履歴情報２１と署名鍵（電子印鑑）２２とを格納する領域を有している。ここで、ユーザファイル１２に記録される履歴情報２１としては、管理センタ１４の図示しない署名鍵により電子署名されたものが記録される。また、署名鍵２２は、電子商取引時にユーザ端末１１から管理センタ１４へ送信される電文に電子署名を行うときに用いられる。

【０００７】さて、以上のように構成された電子決済システムの動作の概略を説明する。電子商取引において決済を行うためには、まず正当なユーザであることを確認する必要がある。このため、管理センタ１４に対して決済要求を行う場合は、ユーザ認証用の電文が必要になる。ユーザ認証用の電文には、ユーザ個々に与えられるＩＤと前回利用したときに管理センタ１４から受信した上述の電子署名付履歴情報２１とが含まれる。そしてその電文全体に対して署名鍵２２により電子署名を行い、例えばユーザ端末１１Ａからネットワーク１３を介し管理センタ１４へ送信する。

【０００８】すると、管理センタ１４の管理装置４１は、このユーザ認証電文を受信してユーザＩＤを確認する。また、ユーザの電子署名も図示しない検証鍵により検証する。そして、ユーザＩＤ及びユーザの電子署名が正常なものと認識すると、次にデータベース４２内のそのユーザに対応するファイルから最終履歴情報を読み出し、受信電文と比較することにより、受信したユーザ認証電文の履歴情報を確認する。そして確認結果が正常な場合、管理装置４１は、ユーザによる種々の電子商取引に伴う決済を許容する。

【０００９】こうしてユーザにより種々の電子商取引が行われかつその決済時点で依然としてそのユーザに残高があることを確認すると、管理装置４１は、この新たな残高情報に対し署名鍵による電子署名を施して最終履歴情報としてデータベース４２内の対応するファイルに記録し、かつその最終履歴情報をネットワーク１３を介して該当ユーザ端末１１Ａに送る。この結果、該当ユーザ端末１１Ａが対応するユーザファイル１２Ａにその最終履歴情報を記録することにより、ユーザファイル１２Ａの履歴情報が更新され、次回の決済時には更新された新たな最終履歴情報がユーザ端末１１Ａから管理センタ１４へ送信される。

【００１０】ところで、こうした電子決済システムでは、ネットワークを介して不特定多数間で電子商取引が行われるため、他人に勝手に利用される恐れがある。図３はこうした不正利用の場合の状況を示す図であり、この図は、例えばユーザＡが使用するユーザファイル１２Ａをユーザ Ｂが不正にコピーしてユーザ端末１１Ｂから決済を行う場合を示している。

【００１１】この場合、コピーされたユーザファイル１２Ａの最終履歴情報は履歴状態①であるとする。また、ユーザＢが不正使用する前にユーザＡが先に自身のユーザファイル１２Ａを使用してステップＳ１で決済要求を行うものとする。この決済要求時には履歴状態①の履歴情報が最終履歴情報としてネットワーク１３を介し管理センタ１４に送られる。この場合、管理センタ１４の管理装置４１は、ステップＳ２でこの最終履歴情報の認証を行い、その認証結果を正常と認識すると、種々の電子商取引に伴う決済を許容し、決済終了後にはデータベース４１内のユーザＡ用のファイルの履歴状態①をステップＳ３で更新し、ステップＳ４で履歴状態②とする。

【００１２】その後、ステップＳ５でネットワーク１３を介してユーザ端末１１Ａに対し決済結果を通知する。この決済結果としては、履歴状態②がユーザ端末１１Ａに送られ、ユーザファイル１２Ａの内容が履歴状態①から履歴状態②に書き換えられる。こうして先にユーザＡが決済を行った後、ユーザＡのファイル１２Ａを不正コピーしたユーザＢによる決済要求がユーザ端末１１Ｂにおいてステップ Ｓ６で行われるものとする。即ち、ユーザＡのコピー情報にそのユーザＡのＩＤを付加すると共にこれらの情報に対し、不正コピーしたユーザＡの署名鍵２２により電子署名を行い決済要求として管理センタ１４へ送信される。この場合、最終履歴情報として履歴状態①の履歴情報がネットワーク１３を介し管理センタ１４に送られることになる。管理センタ１４の管理装置４１は、ステップＳ７でこの最終履歴情報の認証を行うが、このときデータベース４２内の最終履歴情報は履歴状態②となっているため、ステップＳ８で履歴不一致通知をユーザ端末１１Ｂに対して行う。その結果、他のユーザのファイル１２を不正コピーしたユーザＢによる決済を禁止することができる。

【００１３】また、ユーザＡがユーザＢのファイル１２Ｂを不正コピーして先に決済を行って管理センタ１４内のデータベースの履歴状態を①から②へ更新した後、ユーザＢが決済を行うと、ユーザＢの決済行為も同様に禁止される。しかし、このときユーザＢは自身のファイル１２Ｂが不正使用されたことに気づきその使用不可の措置を請ずることができる。また、ユーザＢが自身の使用するファイル１２Ｂの破壊等により、決済要求時に最終履歴情報が管理センタ１４に伝達されず、管理センタ１４からステップＳ８で履歴不一致通知が行われ、従って決済行為が不可となる場合は、ステップＳ９で履歴の更新を行うことにより、履歴状態①をステップＳ１０で履歴状態②にすることができる。

【００１４】即ち、図４に示すように、ユーザＢの使用

するユーザファイル１２Ｂの履歴情報が最初の履歴状態①から最終の履歴状態⑩まで更新されるような場合、ユーザ端末１１Ｂではバックアップファイル１５Ｂに例えば最初の履歴情報（履歴状態①）をバックアップしておく。ここでユーザファイル１２Ｂが破壊され、上述の履歴不一致が管理センタ１４から通知されると、ステップＳ２１でバックアップファイル１５Ｂから最初の履歴情報を読み出し、ステップＳ２２でユーザ端末１１Ｂから管理センタ１４へ送信する。

【００１５】すると、管理センタ１４の管理装置４１では、ステップＳ２３でこの電文に含まれる電子署名の認証等を行い、ステップＳ２４で認証結果が正常となると、データベース４２内のユーザＢに対応する最終履歴情報を示す履歴状態⑩をステップＳ２５で取り出し、ステップＳ２６で履歴の更新情報として該当ユーザ端末１１Ｂへ送信する。この結果、ユーザファイル１２Ｂには履歴状態⑩が最終履歴情報として記録されることから、以降、ユーザファイル１２Ｂを用いた決済が可能になる。

【００１６】図５はこの電子決済システムの動作を示すフローチャートである。このフローチャートに従って本システムの要部動作を説明する。なお、図５（ａ）はユーザ端末１１の動作を、図５（ｂ）は管理センタ１４の動作をそれぞれ示している。商品取引時に例えばユーザＡがユーザ端末１１Ａを用いて決済を行う場合は、まず図５（ａ）のステップＳ３１でユーザ端末１１Ａはユーザファイル１２Ａから最終履歴データ（最終履歴情報２１）を読み出し、これにユーザＩＤを付加する。

【００１７】次にＩＤが付加された最終履歴データにステップＳ３２で署名鍵２２による電子署名を行い決済要求電文として作成する。そしてステップＳ３３でこの決済要求電文をネットワーク１３を介して管理センタ１４へ送信する。その後、管理センタ１４では上述したように、送信した決済要求電文の認証処理等が行われ、認証結果が正常となると種々の商取引に伴う決済時の残高情報等を決済結果電文として端末１１Ａ側に送信する。ユーザ端末１１ＡではステップＳ３４でその決済結果電文の受信の有無を判断し、管理センタ１４からの決済結果電文を受信すると、その電文をユーザファイル１２Ａに記録するファイル更新処理をステップＳ３５で実行する。

【００１８】一方、こうしたユーザ端末１１Ａの動作に応動する管理センタ１４では、ユーザ端末１１Ａから送信される決済要求電文の受信の有無を図５（ｂ）のステップＳ４１で判断する。そして、決済要求電文が受信されステップＳ４１の判定が「Ｙ」となると、ステップＳ４２で認証処理を行う。この認証処理では、上述したように、受信した決済要求電文の署名確認及びユーザＩＤの確認を行うと共に、データベース４２内に格納されているこの端末１１Ａの最終履歴データと、この受信電文に含まれる最終履歴データとの間の一致の有無が確認される。

【００１９】そしてこれらの確認結果が何れも正常でステップＳ４３の判定が「Ｙ」となると、ユーザ端末１１Ａによる種々の電子商取引に基づく決済処理をステップＳ４４で実行し、その処理結果の残高情報に自身の電子署名を付加してデータベース４２内のユーザ端末１１Ａに対応したファイル領域に最終履歴データとして記録する。その後、ステップＳ４５でその最終履歴データを決済結果電文として該当ユーザ端末１１Ａに送信しそのファイル１２Ａを更新させる。

【００２０】一方、ステップＳ４２の認証処理の結果、異常となりステップＳ４３の判定が「Ｎ」となる場合は、その異常が電子署名或いはユーザＩＤの不一致による異常か否かをステップＳ４６で判断し、電子署名或いはユーザＩＤの不一致による異常の場合は、ステップＳ４７でそのユーザＩＤ等をデータベース４２内の別途領域に設けたブラックリストに登録し、以降の使用を禁止させる。

【００２１】電子署名或いはユーザＩＤの不一致による異常ではない場合は、ユーザ端末１２Ａ側の履歴データと管理センタ１４側の履歴データの不一致ということで、ステップＳ４８で履歴データ不一致処理を実行する。その結果、第三者によりファイル１２Ａの内容がコピーされることによって無断で使用される等、ユーザＡ側でその理由が不明な場合はそのファイルを用いた取引停止の処理を直ちにステップＳ４９で実行する。

【００２２】また、ユーザファイルの破損や紛失等、ユーザＡがその理由がわかっている場合については、上述したようにバックアップファイルの履歴データをユーザ端末１２Ａから管理センタ１４へ送信する等の処理を行う。その結果、ステップＳ５０で管理センタ１４から最新履歴データをユーザ端末１２Ａに返送する等の処理を行うことにより、ユーザファイル１２Ａの更新が行われ以降のそのユーザファイル１２Ａを用いた取引が再開される。

【００２３】このように、ネットワークを介した電子商取引における決済時には、ユーザファイル１２内の最終履歴と、管理センタ１４内の最終履歴との一致を確認することにより、その決済を許容するため、電子商取引を行う場合にその利用者を限定することができ、従って高セキュリティを確保できる。また、ユーザファイル１２の破損や紛失等の場合は、バックアップファイルの履歴データをユーザ端末１２から管理センタ１４へ送信することにより、管理センタ１４から返送される最終履歴データを受信しユーザファイル１２の内容を更新する。この結果、以降そのユーザファイル１２を使用して決済を行うことができる。

【００２４】

【発明の効果】以上説明したように本発明によれば、電

子商取引に伴う決済時に端末はユーザファイルの最終履歴情報を管理センタに送信し、管理センタはこのユーザファイルの最終履歴情報とデータベースの最終履歴情報とが一致するときに決済を許容するようにしたので、電子商取引を行う場合に利用者を限定することができ、従って高セキュリティを確保できる。また、予めバックアップファイルを端末に設けて取引履歴情報をバックアップすると共に、管理センタからユーザファイルの最終履歴情報とデータベースの最終履歴情報との不一致が通知された場合、端末はバックアップファイルの取引履歴情報を管理センタへ送信しユーザファイルを更新するようにしたので、ユーザファイル内の履歴データの紛失や破損等が生じた場合でもこれを復旧して決済を行うことができる。また、管理センタは履歴情報に自身の署名鍵を用いて電子署名を行い端末へ送信してユーザファイルに記録させ、端末はユーザファイル内の履歴情報に自身のＩＤを付加すると共にＩＤが付加された履歴情報に自身の署名鍵を用いて電子署名を行い管理センタへ送信し、履歴情報の正否を検証させるようにしたので、電子決済システムにおいてより高度なセキュリティ性を確保できる。

【図面の簡単な説明】

【図１】　本発明を適用した電子決済システムの構成を示すブロック図である。

【図２】　上記システム内のユーザファイルの構成を示す図である。

【図３】　上記システムの第１の動作例を説明する図である。

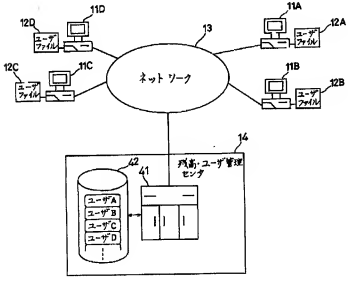
【図４】　上記システムの第２の動作例を説明する図である。

【図５】　上記システムの要部動作を示すフローチャートである。

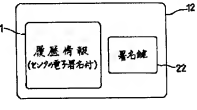
【符号の説明】

１１Ａ～１１Ｄ…ユーザ端末、１２Ａ～１２Ｄ…ユーザファイル、１３…ネットワーク、１４…残高・ユーザ管理センタ、１５Ｂ…バックアップファイル、２１…履歴情報、２２…署名鍵、４１…管理装置、４２…データベース。

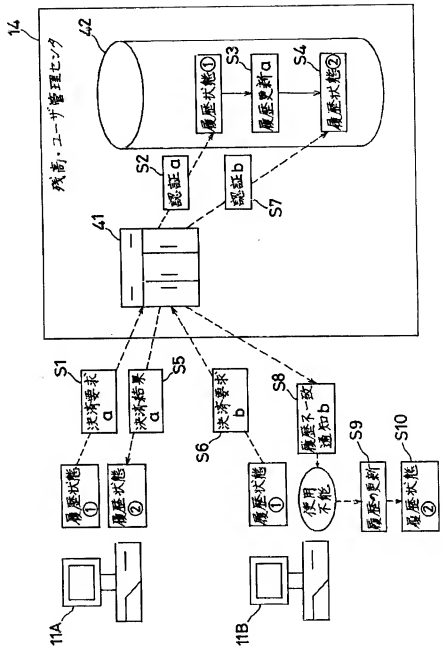
【図１】



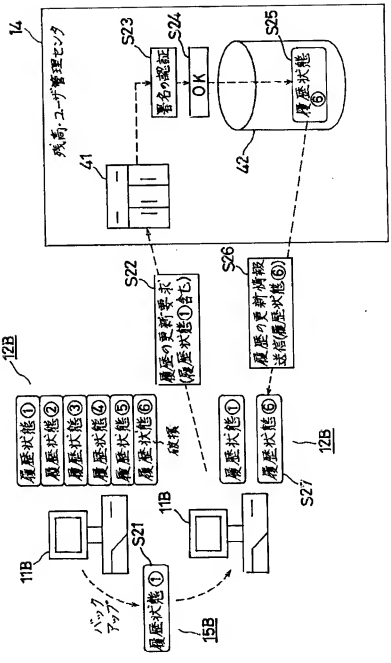
【図２】



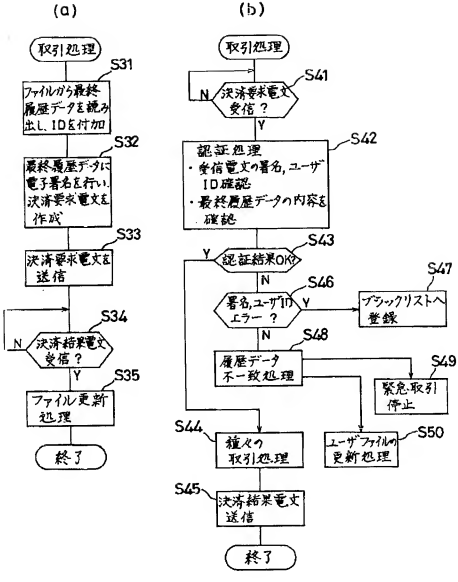
【図3】


14
残高・ユーザ管理ヒンク
42
履歴状態①
履歴更新a
履歴状態②
S3
S4
S2
認証a
認証b
S7
41
S1
決済要求a
決済結果a
S5
決済要求b
S6
S8
履歴不一致通知b
S9
S10
履歴状態①
履歴状態②
履歴状態①
使用不能
履歴の更新
履歴状態②
11A
11B

【図4】


14
残高,ユーザ管理センタ
S23
S24
暗号の認証
OK
S25
履歴状態⑥
41
42
S22
履歴の更新要求
(履歴状態①まで)
S26
履歴の更新情報
送信(履歴状態⑥)
12B
履歴状態①
履歴状態②
履歴状態③
履歴状態④
履歴状態⑤
履歴状態⑥
破棄
11B
S21
バックアップ
履歴状態①
15B
履歴状態①
履歴状態⑥
S27
12B

【図5】


(a)
取引処理
S31
ファイルから最終履歴データを読み出し、IDを付加
S32
最終履歴データに電子署名を行い、決済要求電文を作成
S33
決済要求電文を送信
S34
決済結果電文受信？
N
Y
S35
ファイル更新処理
終了
(b)
取引処理
S41
決済要求電文受信？
N
Y
S42
認証処理
・受信電文の署名，ユーザID確認
・最終履歴データの内容を確認
S43
認証結果OK?
Y
N
S46
署名，ユーザID エラー？
Y
S47
ブラックリストへ登録
N
S48
履歴データ不一致処理
S49
緊急取引停止
S44
種々の取引処理
S50
ユーザファイルの更新処理
S45
決済結果電文送信
終了